Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act

Samuel Kane†

The Computer Fraud and Abuse Act (CFAA) criminalizes a broad range of conduct related to the compromise of computer systems. Specifically, the CFAA prohibits unauthorized access to computer systems, defining such access as that which occurs "without authorization" or in a manner that "exceeds authorized access." Courts interpreting the meaning of unauthorized access under the CFAA have diverged into two camps. On one side, proponents of the broad approach argue that the CFAA unauthorized access inquiry should focus on access purpose, assessing whether a given access was conducted for a purpose authorized by the computer owner. On the other side, proponents of the narrow approach argue that the relevant inquiry should instead be permission focused, looking only at whether the computer owner had granted the accesser permission to access the computer (without regard for why the computer was accessed).

This Comment proposes a three-step framework for assessing CFAA unauthorized access that will resolve the present circuit split. Leveraging concepts from CFAA case law and offering applicability across a wide range of factual and technological contexts, this Comment's Available-Granted-Revoked (AGR) Framework sequentially evaluates (1) whether the computer in question is publicly available or private; (2) whether the computer's owner had, at any point, granted the accesser permission to access the computer; and (3) whether the computer owner had affirmatively revoked the accesser's permission, if any, prior to the purportedly unauthorized access. By adopting the Available-Granted-Revoked Framework, courts will be able to effectively advance the interests underlying both sides of the current circuit split and bring clarity to a persistent legal ambiguity.

† BSFS 2013, Georgetown University; JD Candidate 2021, The University of Chicago Law School. Many thanks to Kelsey Dayton, Jon Fish, Parag Dharmavarapu, Professor Jonathan Masur, and the rest of the *Law Review* staff for their feedback throughout the writing process.

INTRODUCTION

The Computer Fraud and Abuse Act[1] (CFAA) is the federal government's leading computer crime statute, criminalizing a broad range of conduct related to the compromise of computer systems.[2] Specifically, the CFAA prohibits unauthorized access to computer systems, defining such access as that which occurs "without authorization" or in a manner that "exceeds authorized access."[3] Simple, right? Not quite. Let's consider a few examples.

Jim is a computer hacker who hacks into the Alpha Company's database and steals valuable company information. Under the CFAA, this case would be straightforward: Jim's actions would almost certainly constitute access of a computer "without authorization" or in a manner that "exceeds authorized access." Easy.

But let's alter the facts. Suppose Jim is not a hacker, but an Alpha employee. Let's further suppose that Alpha has given Jim access to the database as part of his work duties. Jim decides to quit his job at Alpha, but not before downloading a folder of sensitive company information and forwarding it to the Beta Company, Alpha's chief competitor. Has Jim violated the CFAA? He certainly had access to the database, but did he have authorization when he accessed it for the purpose of sending Alpha's sensitive information to Beta? What if he quit his job, but then accessed the database six months later, using his old login credentials? Different result?

Let's complicate things further by taking our hypothetical out of the employment context. Suppose Alpha has made its database publicly available, accessible to anyone with an Internet connection. Jim is a Beta employee and uses a software tool to scrape data from the public database for Beta's business uses. Did Jim engage in CFAA unauthorized access? The database was publicly available, but does it "exceed authorized access" to run an automated scraper against that information?

As the above examples illustrate, the issue of CFAA unauthorized access is surprisingly complicated, and it is one that courts have struggled to resolve in the decades since the statute's enactment. Generally speaking, courts have divided into a two-sided circuit split. Proponents of the "broad approach"—looking

---

1 Pub L No 99-474, 100 Stat 1213 (1986), codified as amended at 18 USC § 1030.

2 See 18 USC § 1030.

3 See 18 USC § 1030(a), (e)(6) (defining "exceeds authorized access").

to enhance the ability of computer owners to protect their systems—posit that the CFAA unauthorized access inquiry should focus on access purpose, determining whether a given access was conducted for a purpose authorized by the computer owner.[4] Meanwhile, proponents of the "narrow approach"—concerned about the CFAA becoming an overbroad vehicle for criminal liability—have argued that the relevant inquiry should instead be permission focused, looking only at whether the owner had granted the accesser permission to access the computer (without regard for *why* that computer was accessed).[5]

Underlying much of the confusion surrounding the CFAA's unauthorized access provisions is the assumption that this circuit split is fundamentally irreconcilable. In other words, courts must choose to advance the interests of *either* the broad approach's purpose-focused inquiry *or* the narrow approach's permission-focused inquiry.

This Comment rejects that assumption. Instead, it articulates a novel framework that will allow courts to assess CFAA unauthorized access in a manner that protects the interests prioritized by both the broad and narrow approaches. Leveraging concepts from CFAA case law and offering applicability across a wide range of factual and technological contexts, this Comment's Available-Granted-Revoked (AGR) Framework sequentially evaluates (1) whether the computer in question is publicly *available* or private; (2) whether the computer's owner had, at any point, *granted* the accesser permission to access the computer; and (3) whether the computer owner had affirmatively *revoked* the accesser's permission, if any, prior to the purportedly unauthorized access.

This approach serves the interests underlying both the broad and narrow approaches. By limiting the scope of the CFAA's unauthorized access provisions to private computers (via Step 1) and adopting a permission-focused inquiry in Steps 2 and 3, the Framework will help to restrain the scope of CFAA liability—a key aim of narrow-approach advocates. At the same time, by allowing computer owners to terminate access authorization by affirmatively revoking permission (via Step 3), the Framework will advance the broad-approach goal of allowing computer owners to protect their systems.

---

[4] See Part II.B for additional discussion of the broad approach.

[5] See Part II.C for additional discussion of the narrow approach.

This Comment proceeds in three parts: Part I provides an overview of the CFAA, focusing in particular on the statute's unauthorized access provisions. Part II summarizes the current circuit split regarding how broadly or narrowly the CFAA's unauthorized access provisions should be defined. Finally, Part III describes the AGR Framework, applies it to several example cases, and evaluates its benefits and drawbacks.

I. OVERVIEW: THE COMPUTER FRAUD AND ABUSE ACT (CFAA)

Contemporary discussions surrounding the scope of the CFAA's unauthorized access provisions are primarily rooted in debates about what problem(s) Congress intended the CFAA to address and what the statute's text means. Accordingly, Part I.A describes the historical backdrop against which Congress enacted the CFAA, and Part I.B offers a high-level summary of the CFAA's key provisions.

A. Historical Background and Enactment

The late 1970s and early 1980s witnessed growing public concern about the criminal justice system's ability to address computer crime. Prior to this period, computer-related crimes were typically prosecuted under traditional property-crime frameworks.[6] However, commentators criticized this approach, with many observers highlighting the difficulties of applying traditional theft, burglary, and trespass concepts in the digital context.[7] Moreover, the 1970s saw rising levels of public and private computer usage, as well as the entry of computer hackers into the cultural mainstream, further highlighting the property-crime approach's shortcomings.[8]

Acting against this backdrop, Congress enacted the CFAA in 1984,[9] framing it as a response to the inability of existing legal

---

6 See Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 NYU L Rev 1596, 1605–13 (2003).

7 See *Computer Fraud and Abuse Act of 1986*, HR Rep No 99-612, 99th Cong, 2d Sess 5 (1986) (noting that computer data "does not fit well into traditional categories of property"); Kerr, 78 NYU L Rev at 1613–15 (cited in note 6) (summarizing criticisms of the property-crime approach to addressing computer crime).

8 See HR Rep No 99-612 at 4–6 (cited in note 7). Several commentators have also highlighted the role that the 1983 Matthew Broderick film *WarGames* played in raising public awareness of computer hacking. See Jonathan Mayer, *Cybercrime Litigation*, 164 U Pa L Rev 1453, 1458 n 14 (2016) (collecting sources).

9 See *United States v Valle*, 807 F3d 508, 525 (2d Cir 2015). The Act was initially passed as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, then

frameworks to adequately address the growing computer-crime problem.[10] While it is unclear precisely what the bill's drafters viewed as the parameters of computer crime, the congressional reports accompanying the 1984 Act and its 1986 amendments specifically focused on the threat computer hackers posed.[11] For instance, these reports described the Act as prohibiting the computer equivalent of "breaking and entering,"[12] and illustrated the severity of the computer-crime problem by describing incidents involving hackers breaking into computer systems containing financial information and hospital records.[13] These reports thus make clear that, at minimum, Congress intended the CFAA to address the threat of computer hackers.

B. Statutory Overview

The CFAA criminalizes a range of conduct generally related to the compromise of computer systems and offers a civil remedy for entities impacted by such conduct.[14] Most notably, the Act prohibits certain unauthorized access of computers, a concept that encompasses both access "without authorization" and access in a manner that "exceeds authorized access."[15]

The CFAA defines "computer" broadly, encompassing any "electronic, magnetic, optical, electrochemical, or other high

---

amended by the Computer Fraud and Abuse Act of 1986. See Kerr, 78 NYU L Rev at 1598 n 11 (cited in note 6). Several states passed similar laws during this time period as well. See id at 1615–16.

10 See *Counterfeit Access Device and Computer Fraud and Abuse Act of 1984*, HR Rep No 98-894, 98th Cong, 2d Sess 8–10 (1984).

11 See, for example, id at 10–12; HR Rep No 99-612 at 5–7 (cited in note 7).

12 HR Rep No 98-894 at 20 (cited in note 10).

13 See HR Rep No 99-612 at 6 (cited in note 7) (financial records); *Computer Fraud and Abuse Act of 1986*, S Rep No 99-432, 99th Cong, 2d Sess 2–3 (1986) (hospital records).

14 See generally 18 USC § 1030.

15 See, for example, 18 USC § 1030(a)(1)–(2), (4) (prohibiting access both "without authorization" and in a manner that "exceeds authorized access" in a range of contexts). Though unauthorized access can be fairly characterized as the CFAA's primary focus, it is not the only activity the statute prohibits. See, for example, 18 USC § 1030(a)(5)(A) (prohibiting one from "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage . . . to a protected computer"); 18 USC § 1030(a)(6) (prohibiting the trafficking of stolen passwords); 18 USC § 1030(a)(7) (prohibiting extortion schemes involving threats to damage or illicitly obtain information from a protected computer). In addition, it is important to note that "without authorization" and "exceeds authorized access" are not always used in tandem within the statute. Specifically, some CFAA provisions *only* prohibit access "without authorization." For example, 18 USC § 1030(a)(3) criminalizes the actions of an individual who "intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer."

speed data processing device performing logical, arithmetic, or storage functions," as well as "any data storage facility or communications facility directly related to or operating in conjunction with such device."[16] Though several CFAA provisions are applicable only to "protected computers,"[17] that term extends to any computer "used in or affecting interstate or foreign commerce or communication."[18] Courts and commentators view this definition as encompassing "all computers with Internet access."[19]

As a result of Congress's broad conceptualization of "computer," the applicability of the CFAA's unauthorized access provisions is not limited to traditional desktop or laptop computers. For example, courts have applied these provisions in cases involving purportedly unauthorized accesses to websites, on the theory that the servers hosting such websites constitute computers under the CFAA.[20] Thus, the scope of computers subject to the CFAA's unauthorized access provisions is quite expansive.

In sharp contrast to the generally well-understood meaning of computers, courts have split on the meanings of the CFAA's unauthorized access terms—"without authorization" and "exceeds authorized access." With respect to "without authorization," this is unsurprising—the statute simply does not define that term. However, courts have also struggled to apply "exceeds authorized access," which the statute *does* define, albeit somewhat ambiguously, as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[21] This confusion about the meaning of "without authorization" and "exceeds

---

16 18 USC § 1030(e)(1).

17 See, for example, 18 USC § 1030(a)(2)(C), (4)–(5), (7).

18 18 USC § 1030(e)(2)(B).

19 *United States v Nosal*, 676 F3d 854, 859 (9th Cir 2012) (en banc) (*Nosal I*). See also Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 Hamline L Rev 81, 92–93 (2013); Garrett D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 Wm & Mary L Rev 1369, 1384 & n 88 (2011); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn L Rev 1561, 1568 (2010). In addition, some commentators have argued that even an Internet connection might not be necessary to render a computer "protected." See, for example, Kerr, 94 Minn L Rev at 1571 (arguing that "protected computer" covers any machine that has "a microchip or that permits digital storage").

20 See *hiQ Labs, Inc v LinkedIn Corp*, 938 F3d 985, 999 (9th Cir 2019) (characterizing servers as "protected computer[s]" under the CFAA), petition for cert filed (Mar 9, 2020).

21 18 USC § 1030(e)(6).

authorized access" is at the core of the CFAA unauthorized access circuit split, examined in the next Part.

II. CIRCUIT SPLIT: WHAT IS UNAUTHORIZED ACCESS?

Perhaps unsurprisingly, given the statute's lack of definitional clarity, the federal courts of appeals are split regarding the meaning of the CFAA's unauthorized access provisions—namely, the proper interpretation of "without authorization" and "exceeds authorized access."[22] This split features two competing approaches: the broad approach (articulating a more expansive view of the conduct prohibited by these terms) and the narrow approach (asserting a more limited view of the proscribed conduct). At a high level, this split is driven by opposing views regarding whether the CFAA's unauthorized access provisions should account for the purpose of a given access. In other words, courts disagree about whether an access of a computer is unauthorized under the CFAA if the accesser has *permission* to access the computer but does so for a *purpose* of which the computer owner does not approve.

This Part examines the contours of the CFAA unauthorized access circuit split in greater depth. Part II.A begins with a brief review of the CFAA's legislative history, focusing specifically on how that source offers little help in elucidating the meaning of the unauthorized access provisions. Part II.B then discusses the purpose-focused inquiry of the broad approach, while Part II.C examines the permission-focused narrow approach. Part II.D concludes by analyzing two additional concepts—permission revocation and the public/private computer distinction—that have emerged in more recent CFAA unauthorized access cases.

A. (A Largely Unhelpful) Legislative History

The CFAA's legislative history offers little interpretive help in resolving the unauthorized access circuit split. The statute's drafters appear not to have realized that the terms "without authorization" and "exceeds authorized access" would be perceived

---

[22] As of May 3, 2020, the Supreme Court has granted one certiorari petition relevant to the CFAA unauthorized access circuit split, and another is currently pending before the Court. See generally *United States v Van Buren*, 940 F3d 1192 (11th Cir 2019), cert granted, 2020 WL 1906566; *hiQ Labs, Inc v LinkedIn Corp*, 938 F3d 985 (9th Cir 2019), petition for cert filed (Mar 9, 2020). In 2017, the Court denied certiorari petitions pertaining to two relevant Ninth Circuit cases concerning the split. See generally *Nosal v United States*, 138 S Ct 314 (2017); *Power Ventures, Inc v Facebook, Inc*, 138 S Ct 313 (2017).

as ambiguous, resulting in a "sparse legislative record."[23] Moreover, the content that the record *does* include sheds little light on what Congress intended to accomplish with the unauthorized access provisions. Courts and commentators generally agree that in passing the original 1984 version of the statute, Congress was primarily concerned about the threat of computer hacking, which it understood as "trespassing into computer systems or data."[24] The original statute, like the present version, prohibited access "without authorization."[25] However, in place of "exceeds authorized access," the statute penalized one who, "having accessed a computer with authorization, uses the opportunity such access provides for *purposes* to which such authorization does not extend."[26] In the 1986 amendments to the CFAA, Congress replaced that language with "exceeds authorized access."[27] This modification is the source of much of the present confusion surrounding the scope of the unauthorized access provisions—a confusion that the AGR Framework, introduced in Part III.B, is intended to remedy.

There is some dispute about whether the 1984 language actually supports the broad approach's purpose-based view of the CFAA.[28] However, even assuming that it does, analysts disagree about Congress's intent behind the 1986 amendments. Proponents of the broad approach posit that "exceeds authorized access" is merely a rephrasing of the purpose-based inquiry of the 1984 language, while narrow-approach advocates counter that "exceeds authorized access" is an express rejection of that purpose-based view.[29] Unhelpfully, both sides can summon congressional commentary supporting their respective approaches.[30]

---

[23] David J. Rosen, Note, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access"*, 27 Berkeley Tech L J 737, 744 (2012) (noting, for example, that the 1986 Senate Report described the meaning of "exceeds authorized access" as "self-explanatory").

[24] *United States v Valle*, 807 F3d 508, 525 (2d Cir 2015).

[25] Id.

[26] HR Rep No 98-894 at 2 (emphasis added) (cited in note 10). See also Laura Bernescu, Comment, *When Is a Hack Not a Hack: Addressing the CFAA's Applicability to the Internet Service Context*, 2013 U Chi Legal F 633, 638.

[27] *Valle*, 807 F3d at 525.

[28] See, for example, id at 526 (noting that "even when Congress referenced the user's 'purposes,' it spoke in terms of the particular computer files or data to which the user's access rights extended").

[29] Id at 525–26.

[30] For examples summarizing both sides of this debate about the 1986 amendments, see id; Rosen, Note, 27 Berkeley Tech L J at 745 (cited in note 23). A review of primary sources supports commentators' confusion. Compare S Rep No 99-432 at 9 (cited in note 13) (stating that Congress merely intended for "exceeds authorized access" to

Thus, courts have "generally steer[ed] clear of the CFAA's legislative history" in interpreting the statute's unauthorized access provisions.[31]

B. The Broad Approach

This Part examines the broad-approach side of the CFAA unauthorized access circuit split. Part II.B.1 offers an overview of the purpose-focused nature of the inquiry, with Part II.B.2 diving deeper into the question of how broad-approach courts determine whether a given purpose is authorized. Part II.B.3 then evaluates the benefits and drawbacks of this approach.

1. A purpose-focused inquiry.

The First,[32] Fifth,[33] Seventh,[34] and Eleventh[35] Circuits have adopted a broad interpretation of the CFAA's unauthorized access provisions. According to this view, the CFAA's unauthorized access provisions necessitate a purpose-focused inquiry into access—in other words, focusing on whether the accesser accessed a given computer for a purpose authorized by the computer owner.[36] Thus, under the broad approach, the fact that an individual has been granted general permission to access a computer does not necessarily insulate him from CFAA unauthorized access liability.[37]

A brief example helps to illustrate the broad approach's implications. CFAA unauthorized access cases often arise in the employer-employee context,[38] with a typical fact pattern involving

---

"simplify the language" of the 1984 Act), with id at 21 (additional views of Sens Mathias and Leahy) (stating that the amendment would remove from the CFAA's scope "authorized access that aims at purposes to which such authorization does not extend") (quotation marks omitted).

31 Rosen, Note, 27 Berkeley Tech L J at 744–45 (cited in note 23). For additional discussion of the various conflicting purposes underlying the CFAA, see Urban, Note, 52 Wm & Mary L Rev at 1382–92 (cited in note 19).

32 *EF Cultural Travel BV v Explorica, Inc*, 274 F3d 577, 582–84 & n 10 (1st Cir 2001).

33 *United States v John*, 597 F3d 263, 271–72 (5th Cir 2010).

34 *International Airport Centers, LLC v Citrin*, 440 F3d 418, 420 (7th Cir 2006).

35 *United States v Rodriguez*, 628 F3d 1258, 1263 (11th Cir 2010).

36 See, for example, *John*, 597 F3d at 272 (stating that "[a]ccess to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded").

37 See, for example, *Rodriguez*, 628 F3d at 1263 (government employee had general permission to access a database, but was still found liable under the CFAA on the theory that his permission to access the database did not extend to "nonbusiness reasons").

38 See, for example, id at 1260 (federal government employee); *John*, 597 F3d at 269 (financial institution employee); *Citrin*, 440 F3d at 419 (real estate business employee).

some variation of the following chronology: (1) Alpha Company grants employee Jim access to its Database, (2) Jim signs an employment agreement agreeing to only use the Database for business purposes, (3) Jim uses the Database for nonbusiness purposes, and (4) Alpha files suit under the CFAA.[39] A broad-approach court would likely hold that Jim violated the CFAA by exceeding authorized access—while Jim had general permission to access the Database, his access for nonbusiness purposes exceeded the scope of this access authorization. In other words, Jim had permission to access the Database, but used that permission for an unauthorized purpose.

2. What purposes are authorized?

As the above example illustrates, the broad approach hinges on a purpose-based inquiry, asking whether the accesser accessed the computer for a purpose authorized by the computer owner. However, broad-approach courts have adopted differing methods for determining what purposes are authorized in a given scenario.

Generally, the broad-approach courts agree that an individual engages in unauthorized access when he accesses a computer for a purpose that the computer owner expressly prohibited. *United States v Rodriguez*[40] paradigmatically illustrates this approach. In *Rodriguez*, the Eleventh Circuit held that a Social Security Administration (SSA) employee violated the CFAA by accessing SSA databases for nonbusiness purposes (in this case, gathering personal information about various women in order to harass them).[41] In reaching this conclusion, the court claimed to rely on a plain-language interpretation of the CFAA.[42] The SSA, the court noted, maintained a policy prohibiting the nonbusiness use of its databases and communicated this policy to employees through training sessions and notices.[43] Rodriguez's authorization to use these databases, then, extended to business uses

---

[39] A private right of action for monetary damages or injunctive relief is available to "[a]ny person who suffers damage or loss by reason of a violation of [the CFAA]. 18 USC § 1030(g)." This hypothetical roughly approximates the facts of *John*, 597 F3d at 269; *Rodriguez*, 628 F3d at 1260–62; and *Valle*, 807 F3d at 512–13.

[40] 628 F3d 1258 (11th Cir 2010).

[41] Id at 1260–63.

[42] Id at 1263 (arguing that "the plain language of the [CFAA] forecloses any argument that Rodriguez did not exceed his authorized access").

[43] Id at 1260.

only.[44] Thus, by accessing the databases for nonbusiness purposes, Rodriguez necessarily exceeded his authorized access.[45]

Some broad-approach courts have gone further, holding that an individual need not violate an expressly communicated purpose limitation (such as the policy in *Rodriguez*) in order to engage in CFAA unauthorized access. Rather, under this view, courts treat certain access purposes as presumptively unauthorized. The First Circuit offered an early version of this theory in *EF Cultural Travel BV v Explorica, Inc*,[46] which involved a tour company (Explorica) deploying a custom computer program to "scrape" publicly available pricing information from a competitor's (EF Cultural Travel's) website and then using that information to systematically undercut EF's tour prices.[47] There, the court concluded that Explorica's activities likely exceeded its authorized access to EF's website.[48] Though EF's website did not contain any explicit statement prohibiting website users from extracting the site's publicly available data,[49] the court nonetheless concluded that such a use of the website was beyond the scope of what EF *would have* authorized, reasoning that Explorica's use of the EF website "reek[ed]" of unauthorized access.[50]

The Fifth Circuit expanded on this theory in *United States v John*,[51] in which the court held that Dimetriace Eva-Lavon John, a Citigroup employee, violated the CFAA when she used her access to customer-account information to convey that information to her half brother, who used it to make fraudulent charges.[52] The court advanced two lines of argument in justifying this conclusion. First, it adopted a plain-language approach similar to that

---

44 *Rodriguez*, 628 F3d at 1263.

45 Id.

46 274 F3d 577 (1st Cir 2001).

47 Id at 579–80, 583.

48 Id at 582–84. This decision arrived in the First Circuit on appeal from a preliminary injunction that the district court granted against Explorica. Id at 580. Thus, the court did not rule on the merits of the CFAA unauthorized access issue, stating only that EF was "likely to prove such excessive access." Id at 582.

49 See id at 580 & n 6 (noting that the EF website included a copyright symbol, but describing no additional notice prohibiting data scraping).

50 *EF Cultural Travel*, 274 F3d at 583. The court focused on two factors: (1) that Explorica had used an automated data-scraper tool to extract the relevant data; and (2) that that tool was built with proprietary information from a former EF employee. See id. These two realities, the court reasoned, distinguished the instant case from a situation in which, for instance, Explorica had simply manually extracted information from the website through repeated searches. Id.

51 597 F3d 263 (5th Cir 2010).

52 Id at 269.

employed in *Rodriguez*, holding that an employer can limit an employee's authorization to use a computer to specific purposes.[53] Under this standard, John's actions clearly exceeded her authorized access—the court noted that Citigroup maintained policies prohibiting the misuse of customer information and communicated those policies to employees through training programs (which John attended).[54] Second, the court justified its decision on a broader reasoning, suggesting that John's access of the database to perpetrate fraud was presumptively unauthorized. Citing an earlier Fifth Circuit decision[55] for the proposition that courts have analyzed an individual's access authorization through the prism of a computer's "expected norms of intended use," the court concluded that John's access was necessarily unauthorized—surely, perpetrating fraud was not an intended use of the Citigroup database.[56] Moreover, the court argued, even in the absence of an express employer policy prohibiting database misuse, John presumably "ha[d] reason to know" that she was not authorized to access customer information in service of a fraud scheme.[57]

Finally, the Seventh Circuit has adopted the most expansive view of the broad approach, relying on common-law agency principles to hold that an employee's mere acquisition of "adverse interests" is sufficient to strip him of authorization to access the employer's computers.[58] Thus, in *International Airport Centers, LLC v Citrin*,[59] the Seventh Circuit held that an employee who decided to quit his job and proceeded to delete data on his company-provided laptop violated the CFAA.[60] In the court's view, the employee's decision to quit his job and delete the files breached his duty of loyalty to his employer, thereby "terminat[ing] his agency relationship . . . and with it his authority to access the laptop."[61] Given the breadth of this agency-theory

---

53 Id at 272 (stating that "[a]ccess to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded").

54 Id.

55 See generally *United States v Phillips*, 477 F3d 215 (5th Cir 2007).

56 *John*, 597 F3d at 271–72. The court also approvingly cited the First Circuit's idea that certain accesses may simply "reek[ ]" of unauthorized use. Id at 272, citing *EF Cultural Travel*, 274 F3d at 583.

57 *John*, 597 F3d at 273.

58 *Citrin*, 440 F3d at 420–21.

59 440 F3d 418 (7th Cir 2006).

60 Id at 419–21.

61 Id at 420–21.

interpretation, it is perhaps unsurprising that courts have largely not adopted the Seventh Circuit's reasoning.[62]

3. Benefits and drawbacks of the broad approach.

The broad approach allows the CFAA to address an expansive range of computer-based misconduct. One could argue that this broader read of the CFAA is necessary in the face of modern computer crime, which is not limited to the archetypical hacker threat that the statute was originally intended to address. Indeed, modern computer criminals often take the form of "insider threats"—for example, employees utilizing their granted access to undermine their employers' interests. Thus, the broad approach allows organizations to more effectively enforce proper use of their computer systems and thereby protect their proprietary information.[63]

Courts and commentators have criticized the broad approach, however, for essentially allowing private entities to determine what constitutes a CFAA violation. The broad approach is notable in that it allows employment contracts, confidentiality agreements, terms-of-service (TOS) agreements, and similar documents to define the boundaries of authorized access.[64] For instance, under the broad approach, a website owner could theoretically render a given use unauthorized, without any notice to users, merely by changing its TOS agreement.[65] Thus, commentators have suggested that the broad approach may render the CFAA unconstitutionally vague and overbroad, necessitating the adoption of the narrow approach.[66]

---

62 See Annie Lee, Note, *Algorithmic Auditing and Competition Under the CFAA: The Revocation Paradigm of Interpreting Access and Authorization*, 33 Berkeley Tech L J 1307, 1313 & n 36 (2018).

63 Though trade secret law may offer some help in this context, it is far from a perfect solution. Specifically, the type of information stolen by an insider may fail a trade secret statute's economic-value or secrecy-measure requirements, particularly if it is stored on a shared database. For additional discussion of the intersection between trade secret law and the CFAA, see note 117.

64 See, for example, *EF Cultural Travel*, 274 F3d at 583–84 (confidentiality agreement); *John*, 597 F3d at 272–73 (official company policy, reinforced through training programs).

65 See *United States v Nosal*, 676 F3d 854, 862 (9th Cir 2012) (en banc) (*Nosal I*) (noting that "website owners retain the right to change the terms [of service] at any time and without notice").

66 See Jensen, Comment, 36 Hamline L Rev at 84 (cited in note 19) (arguing that "[o]nly a narrow interpretation of the CFAA keeps the statute constitutional").

As Part III will illustrate, the AGR Framework is responsive to the broad approach's goal of allowing computer owners to protect their systems. The Framework's third step, focused on permission revocation, provides a mechanism by which computer owners can achieve this objective: If a computer owner does not like how an accesser is utilizing his granted access, then the owner can simply revoke that accesser's permission and then bring a CFAA action in response to any future accesses. At the same time, however, the Framework imposes important limitations on CFAA liability—for instance, by clearly limiting CFAA unauthorized access liability to private computers (via Step 1) and requiring that revocations under Step 3 be affirmatively made by the computer owner (rather than simply conveyed in, for example, a TOS modification). These limitations, in turn, protect the Framework from the overbreadth criticisms frequently levied against the broad approach.

C. The Narrow Approach

This Section explores the narrow approach to CFAA unauthorized access. Part II.C.1 examines the permission-focused inquiry at the heart of the narrow approach, while Part II.C.2 discusses the approach's benefits and drawbacks.

1. A permission-focused inquiry.

The Second,[67] Fourth,[68] and Ninth[69] Circuits have adopted a narrow interpretation of the CFAA's unauthorized access provisions.[70] Under this interpretation, unauthorized access occurs only when an individual accesses a computer that he does not have permission to access. In other words, the accesser's purpose is irrelevant—according to the narrow approach, individuals do not violate the CFAA merely by using their granted access permission for purposes that contravene organizational policies[71] or violate their duty of loyalty to an employer.[72] Therefore, under the hypothetical discussed at the beginning of Part II.B.1, a

---

67 *Valle*, 807 F3d at 524–28.

68 *WEC Carolina Energy Solutions LLC v Miller*, 687 F3d 199, 204–06 (4th Cir 2012).

69 *Nosal I*, 676 F3d at 862–63.

70 It is worth noting that this interpretation seems relatively ascendant. All of the narrow-approach opinions discussed in this Section were issued in 2012 or later, whereas all of the broad-approach decisions discussed in Part II.B were issued in 2010 or earlier.

71 But see *John*, 597 F3d at 272; *Rodriguez*, 628 F3d at 1260.

72 But see *Citrin*, 440 F3d at 420–21.

narrow-approach court would find that Jim did not violate the CFAA's unauthorized access provisions. Alpha Company had granted Jim permission to access its Database, and that fact is sufficient to result in a finding of no unauthorized access under the narrow approach.

Accordingly, the narrow-approach inquiry focuses on permission, asking whether the accesser had permission to access (or "validly accessed") the computer in question.[73] Thus, the narrow approach, in contrast to the broad approach, greatly minimizes the relevance of the employee's access purpose, so long as the employee had general permission to access the computer. For example, in *United States v Nosal*[74] (*Nosal I*), the Ninth Circuit held that no CFAA unauthorized access occurred when employees of Korn/Ferry (an executive search firm) removed information from Korn/Ferry's confidential databases and passed that information to David Nosal, a former employee looking to start a competing business, even though such actions clearly violated company policies.[75] Similarly, in *United States v Valle*,[76] the Second Circuit held that Gilberto Valle (a New York City Police Department officer) did not violate the CFAA when he used his access to law enforcement databases to view information about a woman he had discussed kidnapping as part of his involvement in an online sex fetish community, even though such access contravened NYPD policies limiting database access to law enforcement purposes.[77]

In reaching these conclusions, the narrow-approach courts relied primarily on the rule of lenity.[78] This principle of statutory interpretation requires that courts interpret ambiguous criminal laws narrowly, so as to "provide fair warning of what constitutes criminal conduct, minimize[ ] the risk of selective or arbitrary enforcement, and strike[ ] the appropriate balance between the legislature and the court in defining criminal liability."[79] The CFAA's

---

73 *Miller*, 687 F3d at 204.

74 676 F3d 854 (9th Cir 2012) (en banc).

75 Id at 856, 864. The Fourth Circuit reached a similar conclusion on similar facts in *Miller*. See *Miller*, 687 F3d at 202, 206.

76 807 F3d 508 (2d Cir 2015).

77 Id at 512–13, 523–28. Notably, the court held that Valle's discussions of kidnapping the woman in question represented mere fantasizing, and thus did not rise to the level of conspiracy to kidnap. See id at 511. Thus, this case is distinguishable from *John*, in which the alleged unauthorized access was in service of a broader criminal scheme. See *John*, 597 F3d at 269–70 (applying the broad approach).

78 See *Nosal I*, 676 F3d at 863; *Miller*, 687 F3d at 205–06; *Valle*, 807 F3d at 523.

79 *Valle*, 807 F3d at 523.

text and legislative history, these courts reason, can plausibly be read as ambiguous (though individual courts differ somewhat regarding the precise degree of that ambiguity).[80] Given an ambiguous statute, then, the rule of lenity demands an interpretation that restricts said statute's scope of liability.[81]

The permission-centric nature of the narrow approach has the corresponding effect of diminishing the importance, for CFAA unauthorized access purposes, of use-restriction policies—for example, employment agreements, information-technology use policies, TOS agreements, and other documents describing how an individual may use a computer. Indeed, narrow-approach courts have essentially rejected the notion (suggested by broad-approach cases like *John* and *Rodriguez*) that an individual can engage in unauthorized access merely by violating a use-restriction policy.[82]

2. Benefits and drawbacks of the narrow approach.

From the perspective of a computer owner looking to protect his computer from malevolent actors, the narrow approach is undoubtedly problematic. After all, by removing purpose from the unauthorized access inquiry, the narrow approach curtails the CFAA's applicability to individuals who use their granted access permissions to engage in conduct contrary to the computer owner's interests. Indeed, in narrow-approach cases, the accesser often acts in knowing violation of express employer prohibitions.[83] Under the broad approach, such actions would almost certainly result in CFAA liability. However, under the narrow approach, the malicious purpose of the access simply does not matter—in

---

80 *Nosal I* and *Miller* reason that the CFAA's text and legislative history support a narrower reading of the Act, even without the rule of lenity. *Nosal I*, 676 F3d at 863 (framing the narrow approach as a "more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking"); *Miller*, 687 F3d at 207 (expressing an unwillingness "to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith"). In contrast, *Valle* offers a more ambivalent view of the text and legislative history's clarity. *Valle*, 807 F3d at 524 (asserting that the CFAA's text is "readily susceptible to different interpretations"); id at 526 (finding "support in the legislative history for both" the broad and narrow approaches).

81 See, for example, *Valle*, 807 F3d at 523 (concluding that "the rule of lenity requires us to adopt the defendant's [narrow] construction").

82 See, for example, *United States v Nosal*, 844 F3d 1024, 1028 (9th Cir 2016) (*Nosal II*) (noting that the Ninth Circuit has "held that authorization is not pegged to website terms and conditions").

83 See, for example, *Nosal I*, 676 F3d at 856 & n 1; *Miller*, 687 F3d at 202; *Valle*, 807 F3d at 513.

the view of these courts, the fact that an individual has permission to access a computer is sufficient to shield them from CFAA unauthorized access liability.

Courts adopting a narrow view of CFAA unauthorized access have justified their approach as helping to limit the scope of the CFAA to that of an "anti-hacking statute," rather than "an expansive misappropriation statute."[84] As suggested above, narrow-approach courts view this limitation of the CFAA's scope as necessitated by a combination of the rule of lenity and the statute's text and legislative history. As an initial matter, narrow-approach courts are generally sympathetic to a reading of the CFAA's unauthorized access provisions as being specifically focused on the hacker threat.[85] However, these courts also argue that, even if it is conceded that the CFAA's text and legislative history is ambiguous, the rule of lenity dictates a narrower interpretation to avoid turning vast swaths of relatively innocent behavior (like checking personal emails on a work computer) into federal crimes "simply because a computer is involved."[86]

This goal of limiting the CFAA's scope is one served by the AGR Framework presented in Part III.B. Steps 2 and 3 of the Framework focus expressly on the granting and revocation of permission, heavily drawing upon the logic of the narrow-approach cases. Moreover, the Framework, leveraging the concept of the public/private computer distinction, extends the logic of the narrow approach to conclude that CFAA unauthorized access cannot occur in the context of a computer that is publicly available.

D. Additional Concepts

Not all CFAA unauthorized access cases can be neatly categorized into the broad- or narrow-approach frameworks. The cases detailed in the previous two sections predominantly took place in the employer-employee context and hinged on analyses of access purpose (for the broad approach) or access permission (for the narrow approach). However, in recent years, circuit courts have decided CFAA unauthorized access cases that took place outside of the employment context and involved analytical considerations other than those of access purpose and access

---

[84] *Nosal I*, 676 F3d at 857.

[85] See, for example, id at 858–59 (characterizing the CFAA's scope as focused primarily on computer hacking).

[86] Id at 860.

permission. In adjudicating these cases, courts have articulated two concepts—revocation and the public/private computer distinction—that earlier discussions of the CFAA unauthorized access circuit split largely ignored. The AGR Framework explained in Part III.B incorporates these concepts into its analytical approach, thus filling a key gap in existing CFAA unauthorized access jurisprudence.

The sections below explore both of these concepts in greater depth. Part II.D.1 discusses the concept of authorization revocation, in particular focusing on initial steps that the Ninth Circuit has taken to define how such revocation can be effectuated. Part II.D.2 examines the distinction between public and private computers, and explores how the CFAA's unauthorized access provisions may apply differently to each type of computer.

1. Revocation.

The cases discussed in Parts II.B and II.C offer extensive discussion of what makes a given access authorized, but largely ignore the question of whether and how such authorization can be terminated. However, the Ninth Circuit has recently outlined a theory of CFAA authorization revocation, which Step 3 of the AGR Framework largely adopts. Specifically, the Ninth Circuit has stated that (1) an individual's authorization to access a computer can be revoked and (2) postrevocation attempts to access that computer, whether through a third party or "technological gamesmanship," can constitute CFAA unauthorized access.[87]

United States v Nosal[88] (*Nosal II*) offers an application of the Ninth Circuit's revocation theory. This case involved the same parties as *Nosal I*.[89] By the time of *Nosal II*, Nosal and two of his accomplices (Becky Christian and Mark Jacobson) had left Korn/Ferry, and Korn/Ferry had revoked their computer access credentials.[90] However, Christian and Jacobson subsequently borrowed credentials from Nosal's former executive assistant and used those credentials to extract information from Korn/Ferry's computer systems.[91] The court held that this conduct constituted access "'without authorization' in violation of the CFAA."[92]

---

87 *Facebook, Inc v Power Ventures, Inc*, 844 F3d 1058, 1067 (9th Cir 2016).

88 844 F3d 1024 (9th Cir 2016).

89 See text accompanying notes 74–75.

90 *Nosal II*, 844 F3d at 1029, 1031.

91 Id.

92 Id at 1038.

Specifically, applying its revocation model, the court held that (1) Korn/Ferry's revocation of Nosal, Christian, and Jacobson's access credentials "unequivocally conveyed" that they had "no authorization to access Korn/Ferry's computer system,"[93] and (2) their subsequent use of the executive assistant's login credentials to access Korn/Ferry's databases therefore amounted to CFAA unauthorized access.[94]

Facebook, Inc v Power Ventures, Inc,[95] decided one week after *Nosal II*, expanded on the Ninth Circuit's revocation model by identifying additional mechanisms (namely, cease-and-desist letters and technical countermeasures) through which authorization can be revoked. In *Power Ventures*, the court considered a case involving Facebook and Power.com, a rival social media site whose business model essentially consisted of allowing users to aggregate their various social media profiles on a single platform.[96] Power launched a promotional campaign that allowed its users to promote Power by clicking a button on its website that, in turn, automatically created a post on the user's Facebook profile.[97] Facebook responded by sending Power a "cease and desist letter" and implementing an Internet Protocol (IP) block "to prevent Power from accessing the Facebook website."[98] Power ignored the cease-and-desist letter and technically circumvented the IP block, thereby allowing it to continue its campaign.[99] The court held that Facebook's cease-and-desist letter constituted a revocation of authorization,[100] and noted that the IP block "further demonstrated that Facebook had rescinded permission for Power

---

93 Id at 1036.

94 *Nosal II*, 844 F3d at 1038. The court also rejected the relevance of the executive assistant having voluntarily provided her access credentials to Christian and Jacobson, stating that she "had no mantle or authority to override Korn/Ferry's authority to control access to its computers." Id at 1035.

95 844 F3d 1058 (9th Cir 2016).

96 Id at 1062.

97 Id at 1063.

98 Id.

99 *Power Ventures*, 844 F3d at 1063.

100 Id at 1069.

to access Facebook's computers."[101] Thus, the court concluded, Power violated the CFAA by engaging in subsequent access.[102]

2. The public/private computer distinction.

The canonical broad- and narrow-approach cases primarily occurred in the employment context, and thus involved what could be characterized as private computers—those not available to the general public.[103] Common sense would suggest that the concept of unauthorized access would apply differently to computers that are publicly accessible. Indeed, some courts have adopted this view, holding that public computers cannot be subject to unauthorized access, a premise that Step 1 of the AGR Framework adopts as well.

For example, in *Pulte Homes, Inc v Laborers' International Union of North America*,[104] the Sixth Circuit held that a labor union did not engage in access "without authorization" when it "bombarded" a construction company's public-facing email system with thousands of emails.[105] In so concluding, the court relied primarily on the publicly accessible nature of the computers in question—in other words, because the company's email systems were open to the public (accessible without the need to use, for example, a password), the union had authorization to access them, even if such access was contrary to the construction company's interests.[106]

---

[101] Id at 1068. In a footnote, the court cautioned that "[s]imply bypassing an IP address, without more, would not constitute unauthorized use," noting the possibility that a blocked user might not realize that he has been blocked, or that he may discover the block and "conclude that it was triggered by misconduct by someone else who shares the same IP address, such as [his] roommate or co-worker." Id at 1068 n 5. Thus, the court seemed to imply that an IP block must be accompanied by some more explicit form of notice (like a cease-and-desist letter) in order to constitute a valid revocation of authorization.

[102] Id at 1068.

[103] It is true that *EF Cultural Travel* involved scraping data from a publicly available website. However, that case also involved an allegation that the relevant data-scraping tool was based, in part, on confidential information that a former EF employee had provided to Explorica. See *EF Cultural Travel*, 274 F3d at 583. This fact thus distinguishes *EF Cultural Travel* from the two cases discussed in this Section, neither of which involve any claimed misuse of confidential information.

[104] 648 F3d 295 (6th Cir 2011).

[105] Id at 299, 304. The construction company raised its unauthorized access claim under 18 USC § 1030(a)(5)(B) and (C), both of which criminalize only access "without authorization." Id at 300. Thus, the court left open the question of whether the union "exceed[ed] authorized access" under the CFAA. See id at 304.

[106] Id at 304.

The Ninth Circuit applied a similar distinction between public and private computers in *hiQ Labs, Inc v LinkedIn Corp*,[107] a recent case involving a dispute between LinkedIn and hiQ, a company that generates data-analytics products based on information it scrapes from LinkedIn users' public profiles.[108] This case reached the Ninth Circuit on appeal from a preliminary injunction (hiQ sought to enjoin LinkedIn from denying it access to the aforementioned profiles), and so the court did not resolve on the merits the issue of whether hiQ's activities constituted CFAA unauthorized access.[109] However, in affirming hiQ's sought-after injunction, the court strongly suggested that hiQ's scraping of public LinkedIn data, even after receipt of LinkedIn's cease-and-desist letter, would not constitute access "without authorization."[110] The key factor driving this conclusion, the court reasoned, was the publicly accessible nature of the scraped data. The data available on public LinkedIn profiles, the court pointed out, "is not owned by LinkedIn and has not been demarcated by LinkedIn as private using" a system "such as username and password requirements."[111] Rather, it is "available to anyone with a web browser."[112] These factors, the court concluded, thus strongly suggest that hiQ's scraping activities do not run afoul of the CFAA's unauthorized access provisions.[113]

Thus, the current state of the CFAA unauthorized access circuit split is essentially as follows: The broad and narrow approaches articulate competing visions of the CFAA unauthorized access inquiry. On the one hand, broad-approach courts employ a purpose-focused inquiry, asking whether an access was made for a purpose authorized by the computer owner, thereby giving computer owners more effective control over the use of their systems. On the other hand, narrow-approach courts, seeking to limit the CFAA's punitive scope, advance a permission-focused inquiry, discarding access purpose and focusing solely on whether the

---

107 938 F3d 985 (9th Cir 2019), petition for cert filed (Mar 9, 2020).

108 Id at 991.

109 Id at 989.

110 Id at 1003–04.

111 *hiQ Labs*, 938 F3d at 1003–04.

112 Id at 1002.

113 Id at 1003–04. The nature of the data involved also distinguishes *hiQ Labs* from *Power Ventures*, which involved Power's access to nonpublic Facebook data. Compare *hiQ Labs*, 938 F3d at 1002, with *Power Ventures*, 844 F3d at 1063 ("Facebook has tried to limit and control access to its website . . . [and] requires third-party developers or websites that wish to contact its users through its site to enroll in a program called Facebook Connect.").

accesser had general permission to access the information in question. However, several recent cases have discussed concepts—namely, authorization revocation and the public/private computer distinction—that have gone relatively unexamined within the canonical circuit-split cases.

The result of all this is a muddled assortment of competing frameworks, concepts, and interests. Given this reality, how can courts evaluate CFAA unauthorized access in a manner that is both consistent with the Act's text and purpose, but also applicable to the increasingly diverse contexts in which parties invoke the Act's unauthorized access provisions? Part III provides an answer.

III. SOLUTION: A NEW FRAMEWORK FOR ASSESSING CFAA UNAUTHORIZED ACCESS

This Part describes, applies, and assesses this Comment's Available-Granted-Revoked Framework. To begin, Part III.A establishes the need for a solution to the unauthorized access circuit split. Then, Part III.B describes each of the Framework's three analytical steps—whether the computer is publicly *available* or private, whether the computer owner has *granted* access permission to the accesser, and whether the computer owner has *revoked* that permission. Next, Part III.C applies the Framework against several example fact patterns, demonstrating the analytical clarity that courts applying the Framework will bring to bear on a range of challenging scenarios. Finally, Part III.D evaluates the drawbacks and benefits of the Framework, ultimately concluding that the latter far outweigh the former.

A. The Need for a Solution

Before describing the Framework's specific components, it is important to establish why a solution to the unauthorized access circuit split is even necessary in the first place. This Section provides answers to this question. To that end, Part III.A.1 summarizes the current state of CFAA case law, characterized by a persistent circuit split and a growing application of the unauthorized access provisions to new factual contexts. Part III.A.2 then outlines the unique role that the CFAA's unauthorized access provisions play in punishing a specific type of computer-related misdeed, and why alternative legal frameworks (such as trade secret law and contract causes of action) cannot fill that role.

1. The continued circuit split and growing application of the unauthorized access provisions in nonemployment contexts.

A survey of existing case law and commentary addressing CFAA unauthorized access yields two observations. First, the meanings of the terms "without authorization" and "exceeds authorized access" remain subject to an active circuit split,[114] though the narrow approach appears to be gaining traction in more recent cases.[115] Second, much of the relevant case law operates within the employment context, typically dealing with situations in which an employee uses granted computer access for purposes contrary to those of his employer. Undoubtedly, unauthorized access issues are prevalent in this arena. However, as Part II.D noted, the unauthorized access issue is becoming increasingly prominent in nonemployment contexts. These cases, in turn, apply novel concepts, like revocation and the public/private computer distinction, that the employment cases have largely ignored.[116]

These observations suggest the potential utility of a new approach to addressing CFAA unauthorized access issues—one that reconciles the two sides of the existing circuit split and resolves disputes in both the employment and nonemployment contexts. The AGR Framework offers precisely such an approach.

2. Continued relevance of the CFAA unauthorized access provisions.

Of course, it is worth considering whether a solution to the unauthorized access circuit split is even necessary. After all, the CFAA's unauthorized access provisions are not the sole mechanism through which individuals can be punished for

---

[114] As stated in note 22, the Supreme Court denied certiorari in *Nosal II* and *Power Ventures*. See *Nosal v United States*, 138 S Ct 314 (2017); *Power Ventures, Inc v Facebook, Inc*, 138 S Ct 313 (2017). However, it recently granted certiorari in *United States v Van Buren*, 940 F3d 1192 (11th Cir 2019), cert granted, 2020 WL 1906566, in which the defendant essentially sought to overrule the Eleventh Circuit's prior decision in *Rodriguez*. See *Van Buren*, 940 F3d at 1207. In addition, as of May 3, 2020, a certiorari petition remains pending with regards to *hiQ Labs*.

[115] As discussed in note 70, all of the narrow-approach decisions were issued in 2012 or later, whereas all of the broad-approach decisions were issued in 2010 or earlier.

[116] See, for example, *Power Ventures*, 844 F3d at 1066–68; *Pulte Homes*, 648 F3d at 303; *United States v Drew*, 259 FRD 449, 461–62 (CD Cal 2009) (concluding "that an intentional breach of [the terms of service] can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization").

computer-related misdeeds. For example, CFAA unauthorized access cases often involve claims associated with trade secret misappropriation,[117] employment-related causes of action (such as breach of contract claims),[118] and CFAA provisions *not* involving unauthorized access.[119] In light of this reality, why not simply allow unauthorized access cases to be governed by the legal frameworks of these alternative causes of action?

Such an approach is tempting, but ultimately unsatisfying. Though the CFAA's unauthorized access provisions overlap with other legal frameworks, they are unique in their focus on allowing computer owners to protect the integrity of their systems. Unlike trade secret laws (activated only when the information in question is a trade secret) or contract causes of action (requiring a contractual relationship), the CFAA's unauthorized access provisions alone police the specific act of an unauthorized access to a computer. For this reason, the unauthorized access provisions are worth saving.

---

[117] See, for example, *Nosal I*, 676 F3d at 856 (noting that "[t]he government indicted Nosal on twenty counts, *including trade secret theft*, mail fraud, conspiracy and violations of the CFAA") (emphasis added). Trade secret misappropriation *may* occur as a result of a CFAA unauthorized access—for example, if an employee engages in an unauthorized access and then steals a trade secret. However, in order for such a theft to constitute trade secret misappropriation, the information stolen must actually be a trade secret, a legal term of art governed by specific requirements. For instance, the Economic Espionage Act of 1996 states that, in order for information to be a trade secret, it must "derive[ ] independent economic value . . . from not being generally known," and be protected by "reasonable measures to keep [the] information secret." 18 USC § 1839. Thus, the fact that an individual steals company information through a CFAA unauthorized access does not necessarily mean that the individual engaged in trade secret misappropriation.

The shortcomings of trade secret law are further highlighted by the fact that many CFAA unauthorized access cases involve information stored on shared databases. See, for example, *Nosal I*, 676 F3d at 856. This reality can make it difficult for employers to establish that they took reasonable measures to preserve the secrecy of the information in question. See Danielle J. Reid, Note, *Combating the Enemy Within: Regulating Employee Misappropriation of Business Information*, 71 Vand L Rev 1033, 1047 (2018). For additional information about the legal frameworks surrounding trade secrets and the protection of business information, see id at 1041–49.

[118] See, for example, *American Furukawa, Inc v Hossain*, 103 F Supp 3d 864, 866 (ED Mich 2015); *Estes Forwarding Worldwide LLC v Cuellar*, 239 F Supp 3d 918, 920–21 (ED Va 2017). See also Urban, Note, 52 Wm & Mary L Rev at 1396–97 (cited in note 19).

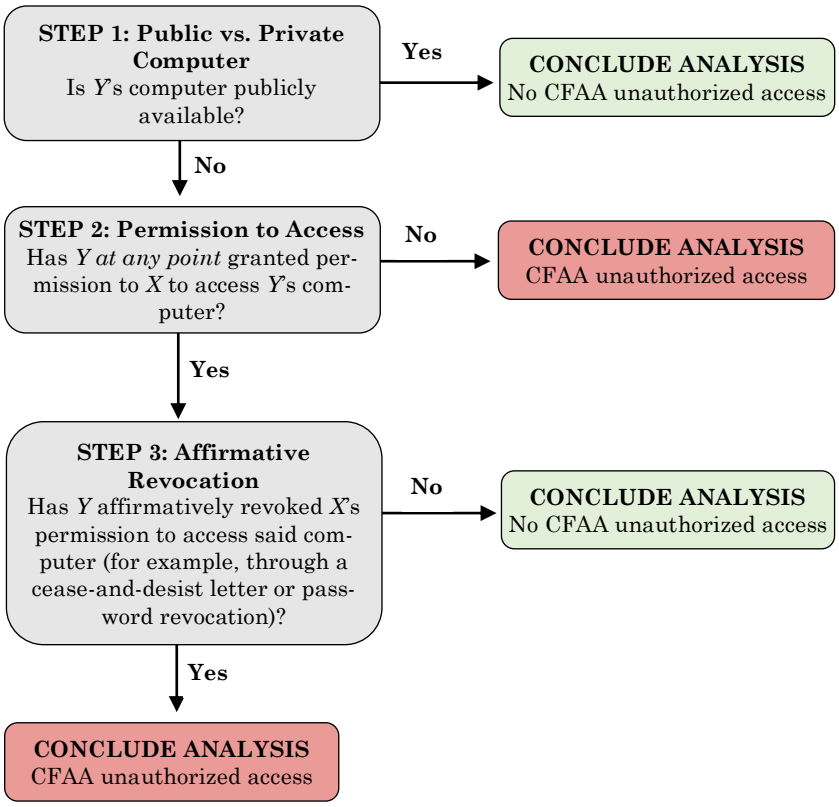
[119] See, for example, 18 USC § 1030(a)(5)(A) (prescribing a punishment for individuals who, inter alia, knowingly transmit code that causes damage to a protected computer); 18 USC § 1030(a)(6) (prescribing a punishment for individuals who traffic passwords); 18 USC § 1030(a)(7)(A) (prescribing a punishment for individuals who transmit extortionary communications threatening to damage a protected computer). The defendant in *John* was convicted of charges under 18 USC § 1029, in addition to his CFAA charges. See *John*, 597 F3d at 283.

B. Defining the Framework

The AGR Framework proposes that unauthorized access under the CFAA be evaluated using a three-step, sequential framework, summarized in the diagram below and explained in greater detail beginning with Part III.B.1. Note that this Section's discussion of each of these steps assumes a factual scenario in which *X* accesses *Y*'s computer (including *Y*'s computer's data).

FIGURE 1: THE AVAILABLE-GRANTED-REVOKED FRAMEWORK

Assume that X *accesses* Y*'s computer. . .*



1. Public versus private computers.

This step considers whether *Y*'s computer is publicly available. If *Y*'s computer is publicly available, then the analysis concludes with a finding that *X* has not engaged in CFAA unauthorized access. If *Y*'s computer is *not* publicly available (in other

words, if *Y*'s computer is a private computer), then the analysis proceeds to Step 2.

Under this standard, a computer that is publicly available cannot be subject to CFAA unauthorized access.[120] Thus, this step reflects the principle, advanced in *Pulte Homes* and *hiQ Labs* but largely ignored in the employment-centric CFAA cases (where the relevant computers are private), that public computers simply lie outside the scope of the CFAA's unauthorized access provisions.[121] Beyond aligning with the holdings of *Pulte Homes* and *hiQ Labs*, this principle is likely consistent with most people's normative intuitions. Simply put, it makes sense that computers made freely available to the public cannot be accessed in an unauthorized manner. Authorization, after all, implies a degree of control over who accesses a computer, and if the entities controlling public computers wanted to limit access, they would not have made them public.

Courts should face minimal difficulties in differentiating between public and private computers. Specifically, courts could assess whether the computer is protected by access permissions (such as username and password requirements).[122] Given that this step is intended largely as a threshold question to determine whether the CFAA unauthorized access provisions apply, such a limited inquiry is likely sufficient.

2. Permission to access.

This step considers whether *Y* has *at any point* granted *X* permission to access the computer. If so, then the analysis proceeds to Step 3. If *Y* has never granted *X* permission to access the computer, then the analysis concludes with a finding of CFAA unauthorized access.

This step is intended to criminalize the actions of the classic hacker, prohibiting an individual from accessing a private computer that he has never had permission to access. Given the

---

[120] As discussed in Part I.B, the CFAA defines "computer" broadly, and courts have treated websites and databases as computers for the purpose of assessing unauthorized access.

[121] See *Pulte Homes*, 648 F3d at 304; *hiQ Labs*, 938 F3d at 1003.

[122] See, for example, *hiQ Labs*, 938 F3d at 1003 (asserting that the CFAA "without authorization" provision is violated "when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer").

CFAA's historical roots as an anti-hacking statute, it is important that the Framework proscribe such behavior.

Granted, one could certainly imagine definitional issues arising as courts apply this step. For example, litigants may contest the definition of permission. However, this concern can likely be addressed by referring back to Step 1, which requires that a computer be protected by an access permission system (such as a password) in order to qualify as a private computer protected by the CFAA. Thus, Step 2 can, in turn, define "permission" as the owner-granted ability to access a private computer. Similarly, litigants may challenge the scope of permissions granted. For example, if *Y* grants *X* permission to access a database with five components, a litigant may question which components *X* had permission to access. The short answer, in keeping with Step 2's focus on addressing the hacker threat, is any component that *X* was technically *able* to access, using his granted permissions.[123]

It is important to note that the Framework's conception of permission in Step 2 is one in which permission is bounded by what the accesser is *technically* able to access. To return to Jim's case as an example, his permission to access a computer is defined by what information he is *technically* able to access, not by what Alpha Company *says* he can access. Thus, if Alpha tells Jim that he can only access Database A, but the password that Alpha assigned Jim to use in accessing Database A also allows him to access Database B, then a court applying the AGR Framework would find no unauthorized access for Jim's access of Database B. As this example illustrates, the scope of permission granted under Step 2 is primarily a question of what the accesser is technically able to access.

Granted, the AGR Framework's conception of permission is one that places a greater burden on the computer owner than does the broad approach. However, this burden is a justified one. First,

---

[123] It is worth briefly discussing the possibility of unintentionally granted permission. One could imagine a scenario in which, for example, *Y* grants a group of individuals access to a database, but accidentally includes *X* in that group. The Framework would treat this as granted permission under Step 2. Broadly speaking, the Framework is intended as a relatively objective approach to the issue of CFAA unauthorized access, rather than one focused on the subjective perceptions of computer owners and accessers. For example, consider how Step 3's revocation analysis, discussed below, eschews the amorphous agency analysis of *Citrin* for more objective indicia of permission termination, such as cease-and-desist letters, password revocations, and technical countermeasures. See *Citrin*, 440 F3d at 420–21. Thus, treating an accidental grant of permission as a valid grant of permission aligns with the broader aims of the Framework.

the Framework's safeguard-focused conception of permission is one that helps to facilitate notice to accessers. By requiring that permission be bounded by technical safeguards, the Framework avoids situations in which an individual is faced with CFAA liability for inadvertently accessing a computer that he does not have express consent to access (for instance, if Jim accidentally accessed Database B using the password that Alpha provided him). Second, if computer owners want to deem certain computers off-limits without implementing technical safeguards, they remain free to do so under the AGR Framework, albeit outside of the CFAA's protection. For instance, an employer could incorporate such limitations into its employment agreements. The AGR Framework simply forecloses the possibility of such an agreement then being used as the basis for criminal liability under the CFAA.

3. Affirmative revocation.

The Framework's final step considers whether *Y* has affirmatively revoked *X*'s permission to access the computer. If *Y* has made an affirmative revocation, then the analysis concludes with a finding of unauthorized access. If *Y* has not made an affirmative revocation, then the analysis concludes with a finding of no unauthorized access.

This step, incorporating concepts articulated in *Nosal II* and *Power Ventures*, is aimed at the actions of individuals who *had* permission to access a computer, but had that access revoked by the computer owner. Specifically, Step 3 provides the means for a computer owner to "close[ ] both the front door and the back door" to individuals that it no longer wants to have access to its computers, with former employees and cease-and-desist recipients being prime examples.[124] Step 3 accomplishes this objective in a manner that advances the goals of both the broad and narrow approaches. Consistent with the broad approach, Step 3 allows computer owners to control who has access to their computers. However, Step 3 also limits this power in two important ways.

First, Step 3 mandates the provision of notice to the unauthorized accesser. In order to establish an affirmative revocation, the computer owner will have to clearly indicate to the accesser—through measures either explicitly communicative (like a cease-and-desist letter), technical (like an IP block), or a combination of

[124] *Nosal II*, 844 F3d at 1028.

both (like a password revocation)—that his access is no longer authorized.[125] Under such a framework, the scope of impermissible behavior becomes much clearer, for both the accessers and courts. For instance, rather than engaging in a nebulous analysis of when an employee acquires interests adverse to those of his employer (as seen in cases like *Citrin*), courts will simply look to whether a purportedly unauthorized access occurred after an affirmative revocation took place.

Second, Step 3 avoids the "parade of horribles" often described by critics of the broad approach by removing access purpose from the CFAA unauthorized access inquiry.[126] Thus, the employee who violates his company's computer-use policy by playing online sudoku and the online dater who breaches Tinder's TOS agreement by lying about his height would not face CFAA unauthorized access liability merely because their access was for an impermissible purpose.[127] In these cases, the computer owners would be free to revoke the users' access authorizations; however, they could not dictate specific uses, at least in a manner enforceable by the CFAA's unauthorized access provisions.

A key point of contention in implementing this step will be defining the parameters of "affirmative revocation." The case law suggests a few methods that would likely qualify, including cease-and-desist letters[128] and the revocation of login credentials.[129] While a full-scale cataloguing of permissible methods of affirmative revocation lies outside the scope of this Comment, it stands to reason that the incremental development of such parameters lies well within the institutional competencies of the judiciary.

---

[125] As *Power Ventures* suggests, a computer owner will ideally convey its revocation of authorization through multiple avenues. See *Power Ventures*, 844 F3d at 1068 (noting that Facebook's imposition of an IP block on Power "further demonstrated" the revocation of authorization conveyed by a cease-and-desist letter).

[126] See *Nosal I*, 676 F3d at 860–62 (listing potential far-reaching negative consequences of the broad approach); id at 866 (Silverman dissenting) (describing the majority's list as a "parade of horribles").

[127] See id at 860–62 (majority) (describing how those hypotheticals would be treated under the broad approach). This is not to say, of course, that the Framework would render such company policies powerless. For example, the employee could still face workplace sanctions, and the Tinder user could have his account suspended. The Framework merely precludes the possibility of bringing CFAA charges against these individuals.

[128] See, for example, *Power Ventures*, 844 F3d at 1067–68.

[129] See, for example, *Nosal II*, 844 F3d at 1036. In addition, *Power Ventures* lends some support to the idea that the imposition of technical countermeasures (such as IP blocks) may indicate a revocation of permission, but suggests that such measures must be accompanied by something "more" to communicate to the blocked party that it, specifically, has been blocked. See *Power Ventures*, 844 F3d at 1068 & n 5.

C. Applying the Framework

This Section applies the AGR Framework to several of the cases discussed in Part II, with the goals of demonstrating how courts would practically apply the Framework, comparing the Framework's results with those of the deciding courts, and discussing adjudicative challenges that courts implementing the Framework would encounter. After a brief examination of the classic hacking scenario in Part III.C.1, this Section proceeds to evaluate the narrow-approach, revocation, and public-computer cases in Part III.C.2, followed by the broad-approach cases in Part III.C.3.

As this Section illustrates, application of the Framework generally yields results consistent with those in the narrow-approach, revocation, and public-computer cases. However, the Framework's results diverge from those in several of the broad-approach cases.

1. Classic hacking.

A court applying the Framework to a classic hacking case would deem this scenario a CFAA unauthorized access. The computer in such a scenario would presumably be private (Step 1), and the hacker presumably never had permission to access the computer (Step 2). Given the outcome of Step 2, analysis of Step 3 would be unnecessary.

2. Narrow-approach, revocation, and public-computer cases.

a) Nosal I. A court applying the Framework would find no CFAA unauthorized access, consistent with the Ninth Circuit's conclusion. First, the confidential, password-protected Korn/Ferry database would constitute a private computer. Second, Nosal's accomplices had permission to access the database, as they were still Korn/Ferry employees at the time of the conduct in question. Third, Korn/Ferry had not, at that point in time, revoked the accomplices' access. Thus, a court would find no CFAA unauthorized access.[130]

b) Power Ventures. A court applying the Framework would find CFAA unauthorized access, consistent with the Ninth

---

[130] See *Nosal I*, 676 F3d at 866. A court applying the Framework against the facts of *Valle* would reach a similar result. See Part II.C.1.

Circuit's conclusion. As a threshold matter, the servers hosting Facebook users' password-protected profiles would constitute private computers.

Step 2's permission analysis is more complex in *Power Ventures* than in previous examples, as this case involved split permissions, with two entities (Facebook itself and individual Facebook users) conceivably having the ability to give Power permission to access the private computers in question.[131] It seems reasonable to conclude that Power had permission from Facebook's users to access their private profiles (a sentiment shared by the Ninth Circuit),[132] but no such permission from Facebook itself. This, in turn, raises the question of whether an entity (in this case, a Facebook user) that has permission to access a computer (in this case, Facebook's servers) can then provide permission to another entity (in this case, Power) to access that same computer.[133]

Ultimately, it seems sensible to conclude that accessers who have permission to access a computer from the computer's owner should *not* be able to transfer their permission to individuals to whom the computer owner has not given permission. This conclusion is consistent with the Framework's objective of allowing computer owners to control (to an extent) who is able to access their computers. Allowing an authorized accesser (like the Facebook users in *Power Ventures* or the executive assistant in *Nosal II*) to grant access permission for a computer that they do not own would seem fundamentally at odds with this objective—effectively diffusing the computer owner's permission-granting power to anyone to whom the owner has already granted permission.[134] An analogy to a noncomputer context is illustrative. If I give you a key to my house (in other words, permission to enter), surely I have not automatically given you the authority to then extend

---

131 See *Power Ventures*, 844 F3d at 1068 (describing split permissions).

132 See id at 1067 (arguing that by clicking a button that allowed Power to disseminate messages through their Facebook profiles, the users "took action akin to allowing a friend to use a computer or to log on to an e-mail account"). From this premise, the court concluded that, because of the presumed permission from Facebook users, Power "reasonably could have thought" that it had permission to access Facebook's computers. Id.

133 A similar fact pattern arose in *Nosal II*, in which Nosal argued that his former executive assistant, by relaying her login credentials to his accomplices, had provided him with authorization to access the Korn/Ferry databases. See *Nosal II*, 844 F3d at 1035–36.

134 Here, it is worth recalling that the CFAA defines "computer" as a physical device. See 18 USC § 1030(e)(1). Thus, in a case like *Power Ventures*, the computer in question is the server on which Facebook profiles are hosted, *not* the profile itself. Thus, Facebook, not the Facebook user, is best characterized as the computer owner.

that permission to other people without my knowledge. Allowing split permissions would essentially result in this kind of problematic reality in the CFAA context.

Given the above, a court applying the Framework would hold that Power did not have permission to access Facebook's computers and therefore find CFAA unauthorized access. Even assuming that Power had permission to access Facebook's computers, however, Step 3 would still dictate a finding of unauthorized access, as Facebook affirmatively revoked Power's authorization by sending a cease-and-desist letter and implementing an IP block.

c) Nosal II. First, the relevant computer—Korn/Ferry's confidential database—is clearly a private computer. Second, the accessers (in this case, Christian, Jacobson, and, by extension, Nosal) at one point had permission to access these databases while employed by Korn/Ferry. Third, however, Korn/Ferry had affirmatively revoked these individuals' access authorizations by terminating their login credentials upon the end of their respective employments. Thus, a court applying the Framework would find CFAA unauthorized access, consistent with the Ninth Circuit's conclusion.

As an illustration of the Framework's application, it is worth considering how a court applying the Framework would adjudicate this case had Nosal's executive assistant accessed the database herself (instead of providing her credentials to Nosal's coconspirators) and extracted Korn/Ferry's confidential information to provide to Nosal and company. In this scenario, Steps 1 and 2 would be applied identically as compared to the actual facts—the computer remains private and the accesser (the executive assistant, in this case) had permission to access the computer. However, Step 3 would come out differently—unlike Nosal, Christian, and Jacobson, the executive assistant had *not* had her access to the computer revoked, as she was still employed by Korn/Ferry. Thus, the court would find no CFAA unauthorized access. While this exposes the Framework to some of the same critiques leveled at the Ninth Circuit's actual approach (namely, focusing on the puzzling notion that Nosal would be CFAA liable if he used the executive assistant's credentials to access the database himself, but *not* if he directed the executive assistant to access the database and then relay him the relevant information),[135] it is

[135] See, for example, Jamie L. Williams, *Automation Is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 BU J Sci & Tech L 416, 433 (2018).

important to note that the executive assistant would still be subject to sanctions, whether criminal (for example, for theft of trade secrets) or otherwise (for example, losing her job).

d) hiQ Labs and Pulte Homes. Neither of these cases would proceed past Step 1, as both involved public computers (publicly available LinkedIn profiles and a publicly available email address, respectively).

3. Broad-approach cases.

a) Citrin. A court applying the Framework would find no CFAA unauthorized access. First, the computer in *Citrin* (an employer-provided laptop) is clearly a private computer. Second, Citrin had permission to access this computer as part of his employment. However, at the time of the alleged unauthorized access (Citrin deleting data from the laptop), his employer had not affirmatively revoked Citrin's access to the laptop. Thus, Step 3 of the Framework would dictate a finding of no CFAA unauthorized access.

This conclusion differs from that reached by the court in *Citrin*. However, this divergence is not overly troubling—after all, *Citrin* relied on an agency-theory justification that has been largely limited to the Seventh Circuit.[136]

b) John. A court applying the Framework would find no CFAA unauthorized access. First, the relevant computer (databases containing financial institution customer information) was private. Second, John had permission to access this computer as part of her employment by Citigroup. Third, Citigroup had not, at the time of the relevant accesses by John, affirmatively revoked John's access—thus, Step 3 would dictate a finding of no unauthorized access.

Again, this conclusion departs from the holding of the deciding court. Critics of the Framework will highlight such a result as absurd—after all, John was using company computers to further a criminal fraud scheme.[137] From a normative perspective, it seems preposterous that such conduct should go unpunished. However, such a critique is misleading, for John would not go unpunished. As the Fifth Circuit's opinion made clear, John was also

---

[136] See Lee, Note, 33 Berkeley Tech L J at 1313 (cited in note 62).

[137] See *John*, 597 F3d at 269.

convicted by a jury on an indictment including several counts pertaining to access-device fraud.[138]

This policy point is worth emphasizing. There will certainly be situations in which the Framework will result in malicious actors *not* being punished under the CFAA's unauthorized access provisions. However, one need not worry that these actors will escape entirely unpunished—in many such cases, those individuals will face other forms of criminal liability.[139] Ultimately, the CFAA offers a legal sanction uniquely focused on unauthorized access, and it should not be stretched to function as a gratuitous sentence enhancer for all criminals whose crimes happened to involve a computer.[140]

c) EF Cultural Travel. Here, the relevant "computer" was EF's publicly available website. Thus, Step 1 would dictate a finding of no CFAA unauthorized access.[141]

D. Evaluating the Framework

The Framework is not a perfect solution to the CFAA unauthorized access dilemma. Though it undoubtedly advances the interests underlying both the broad and narrow approaches, it still, in the end, represents a middle ground, and therefore entails certain compromises and tradeoffs. That being said, the Framework offers benefits that outweigh the interests shortchanged by its analytical approach.

1. Framework drawbacks.

The Framework presents two drawbacks—namely, a lack of consideration for access purpose and the need for additional definition of certain key concepts—that, while not crippling to its viability, merit further discussion.

---

138 Id.

139 See, for example, the legal frameworks discussed in Part III.A.2.

140 A court applying the Framework against the facts of *Rodriguez* would reach similar results as those reached in applying the Framework to the facts of *John*. See text accompanying notes 51–57.

141 This analysis is somewhat complicated by the fact that Explorica utilized nonpublic, confidential information from a former EF employee to more efficiently interpret information scraped from the site. However, this reality should not dictate an alternative Step 1 conclusion. Step 1 is, after all, narrowly focused on the public/private nature of the accessed computer (in this case, EF's website). Instead, Explorica's use of confidential information from the former EF employee could be addressed through mechanisms like trade secret law or contract claims.

First, the Framework removes analysis of access purpose from the CFAA unauthorized access inquiry. In other words, in considering whether *X*'s access of *Y*'s computer was authorized, the Framework does not consider *why X* accessed *Y*'s computer. As suggested above, this disregard for access purpose plays an important role in helping to limit the scope of conduct criminalized by the CFAA's unauthorized access provisions. However, the removal of access purpose as a factor of consideration is not without its downsides.

Primarily, its lack of consideration for access purpose means that the Framework does not punish the actions of the "insider threat"—an individual who has permission to access a private computer but uses that access for purposes contrary to the computer owner's interests. So long as computer owners do not affirmatively revoke insiders' authorizations, insider access of said computers, even for malicious purposes, would not run afoul of the Framework. Given large organizations' ever-growing reliance on complicated information-technology infrastructures, the specter of the insider threat is a prominent one.[142] In such a threat environment, organizations would undoubtedly prefer to have the CFAA's unauthorized access provisions available to deter these actors. Of course, the mere fact that computer owners would prefer more draconian criminal sanctions is an insufficient reason to adopt an expansive interpretation of CFAA liability. Moreover, as Part III.B illustrated, the Framework leaves computer owners with mechanisms like permission revocation to control access to their systems.

More generally, the Framework would allow certain normatively "bad" actors, like the fraudster in *John* or the harasser in *Rodriguez*, to go unpunished, at least by the CFAA's unauthorized access provisions. However, as noted previously, it is important to recognize the CFAA's inherent limitations. The Act is not an all-purpose tool for punishing every instance of bad behavior that happens to involve a computer. Other legal avenues exist to punish many of these bad actions.[143] Moreover, under the Framework, a computer owner always has the prerogative to terminate an objectionable use by affirmatively revoking an accesser's authorization. And finally, limiting the scope of the CFAA's

---

[142] See, for example, US Department of Homeland Security, National Cybersecurity and Communications Integration Center, *Combating the Insider Threat* *1–3 (May 2, 2014), archived at https://perma.cc/77FD-SAFV.

[143] See Part III.A.2.

criminal sanctions conforms with the rule of lenity, as several of the narrow-approach courts have noted.[144]

Second, in practice, application of the Framework will require further clarification of certain key definitions (for example, the public/private computer distinction, the meaning of "permission," and valid methods of affirmative revocation). In some cases, of course, existing case law sheds light on how these terms should be defined;[145] however, courts will undoubtedly have to further parse these terms. Nonetheless, this concern should not be considered fatal to the Framework's viability—after all, interpreting ambiguous terms and concepts is well within the judiciary's institutional competencies.

2. Framework benefits.

The Framework offers several contributions to the existing case law and discourse surrounding the CFAA unauthorized access provisions, namely: (1) advancing the interests underlying both the broad and narrow approaches, (2) providing a model applicable across a range of factual and technological contexts, and (3) offering an analytical method consistent with the CFAA's text and purpose.

First, the Framework helps to resolve the existing unauthorized access circuit split in a manner that advances both the broad and narrow approaches' interests. Discussion surrounding the unauthorized access circuit split often suggests that the two approaches—the broad approach's purpose-based inquiry and the narrow approach's permission-based inquiry—are fundamentally incompatible.[146] However, as Parts II.B and II.C illustrated, a closer examination of the broad and narrow approaches indicates that they are driven by interests (enabling computer owners to better protect their computers and limiting the CFAA's scope, respectively) that are by no means mutually exclusive. Arguably, both the broad and narrow approaches suffer from analytical tunnel vision, focusing on select interests advanced by the CFAA to the exclusion of others. The narrow-approach courts explicitly levy this criticism at their broad-approach counterparts. For

144 See notes 78–81 and accompanying text.

145 See, for example, *Power Ventures*, 844 F3d at 1068 (lending support for recognizing cease-and-desist letters and IP blocks as valid methods of affirmative revocation); *Nosal II*, 844 F3d at 1036 (same, but for revocation of login credentials).

146 See, for example, Jensen, Comment, 36 Hamline L Rev at 84–85 (cited in note 19) (positing an either-or choice between the broad and narrow approaches).

instance, the Ninth Circuit has criticized the broad-approach courts for focusing "only [on] the culpable behavior of the defendants before them," thereby failing to consider the larger implications of their expansive interpretation of CFAA liability.[147] However, the narrow-approach courts are guilty of a similar myopia—in their zeal to limit the CFAA's scope, they neglect the interests that the broad approach's more expansive read of the CFAA advances.

Ultimately, both sides of the circuit split miss the reality that the interests underlying the broad and narrow approaches are, in fact, reconcilable—a reconciliation that the AGR Framework delivers. For narrow-approach advocates, the Framework offers a restrained conception of the CFAA unauthorized access provisions' scope. Under the Framework's model, the statute only imposes liability when a private computer is involved (Step 1), and then only when an accesser accesses a computer that either he never had permission to access (Step 2) or for which his access permission had been affirmatively revoked (Step 3). Meanwhile, for broad-approach advocates, Step 3's permission-revocation analysis will ensure that computer owners retain the ability to exert control over who has access to their systems. Admittedly, the Framework requires that computer owners exert this control in a more proactive manner than they would under the broad approach. For example, Step 3 requires that the owner affirmatively revoke access through a mechanism like a cease-and-desist letter, password revocation, or technical countermeasure, rather than by simply burying use prohibitions in a TOS agreement.[148] Nevertheless, though Step 3 may require more affirmative monitoring from computer owners, it still provides them with a mechanism to ultimately control who accesses their systems.[149]

Second, the Framework articulates a model that can be applied in diverse factual and technological contexts. As discussed in Part II.D, the CFAA's unauthorized access provisions are increasingly being applied outside of the employment context in which they have historically been invoked. The Framework acknowledges this trend, providing an approach to the

---

147 *Nosal I*, 676 F3d at 862.

148 See Part III.B.3 for additional discussion of Step 3.

149 It is also worth reiterating that, even if a court's application of the AGR Framework renders the CFAA inapplicable in a given case, the computer owner can still pursue any number of non-CFAA remedies in response to computer-related misconduct (for example, contract or trade secret claims).

unauthorized access inquiry based on concepts—public/private computers, permission, and affirmative revocation—that are largely context and technology neutral. Moreover, the Framework incorporates the concepts of the public/private computer distinction and affirmative revocation, both of which have surfaced in case law and academic commentary, but have remained largely ignored within the foundational cases defining the unauthorized access circuit split. As a result, the Framework can address a wide range of analytical challenges, spanning different types of fact patterns (both within and outside of the employment context) and technology scenarios (whether they be traditional database access cases, like *Valle* and *Rodriguez*, or more novel cases, like *hiQ Labs* and *Power Ventures*).

Third, the Framework delivers the aforementioned benefits in a manner consistent with the CFAA's text and purpose. As discussed in Part I.B, the CFAA's definitions of the two terms foundational to its unauthorized access provisions—"without authorization" and "exceeds authorized access"—are either nonexistent (for the former) or largely unhelpful (for the latter). The Framework remedies this gap, offering courts a simple model that synthesizes concepts from post–CFAA enactment case law to flesh out the minimal definitional guidance offered in the CFAA's text.[150] The Framework is similarly consistent with the Act's purpose, regardless of which of the prevailing views regarding this purpose one adopts. At the broadest level, there is little doubt that Congress intended to construct a more robust legal regime for addressing computer crime.[151] The AGR Framework, by clarifying core CFAA provisions, undeniably aligns with this purpose. Moreover, the AGR Framework also serves the CFAA purposes advocated by both sides of the present circuit split. For those who posit that the CFAA was intended to focus specifically on the

---

[150] By limiting the power of computer owners to define unauthorized access, the AGR Framework can also be justified as helping courts to apply the principle of constitutional avoidance in the CFAA context. A common criticism of the broad approach is that it renders the CFAA unconstitutionally vague by (1) failing to provide individuals with sufficient notice of what behavior is prohibited and (2) encouraging arbitrary and selective enforcement. A narrower interpretation of the CFAA, critics argue, is thus necessary in order to render the CFAA constitutional. See, for example, Jensen, Comment, 36 Hamline L Rev at 115–19 (cited in note 19). See also Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv L Rev 751, 755–57 (2013) (summarizing relevant case law and academic commentary).

[151] See, for example, S Rep No 99-432 at 2 (cited in note 13) (noting that "existing criminal laws are insufficient to address the problem of computer crime").

computer-hacker threat,[152] the AGR Framework provides a solution: Step 2 of the AGR Framework is tailored specifically to address the hacker threat. Meanwhile, for those who argue that the CFAA is also meant to encompass the actions of the insider threat,[153] Step 3 of the Framework offers a way for computer owners to assert control over their systems in response to such concerns.

Ultimately, these benefits vastly outweigh the drawbacks discussed in the previous Section. For the cost of a reduced emphasis on access purpose and a need to flesh out some concepts, the Framework will offer courts an analytical model that advances the interests underlying both sides of the present circuit split, is adaptive to new fact patterns and technologies, and aligns with the statute's text and purpose.

CONCLUSION

The CFAA is almost forty years old. It was passed at a time when the concept of computer crime was in its infancy and the idea of the "computer hacker" was just entering the cultural mainstream. Unsurprisingly, the nature of computer crime has evolved since then, raising questions about precisely what threats the CFAA is intended to address. It is this debate that has given rise to the present circuit split regarding what it means under the CFAA to access a computer "without authorization" or in a manner that "exceeds authorized access."

This Comment provides a novel answer to that decades-old question. The AGR Framework offers an analytical model to resolve the unauthorized access circuit split, asking (1) whether the computer in question is publicly *available* or private; (2) whether the computer's owner had, at any point, *granted* the accesser permission to access the computer; and (3) whether the computer owner had affirmatively *revoked* the accesser's permission, if any, prior to the purportedly unauthorized access. Ultimately, the Framework articulates a model that advances the interests of both the broad and narrow approaches—preserving computer-system integrity and appropriately limiting the CFAA's scope—and is applicable across a range of factual and technological

---

[152] For legislative materials suggesting the focus was on the computer-hacker threat, see HR Rep No 99-612 at 5–6 (cited in note 7); HR Rep No 98-894 at 10–11 (cited in note 10).

[153] See Part III.D.1 for additional discussion of this view.

contexts. In this way, the Framework will help to ensure the CFAA unauthorized access provisions' continued viability, thereby preserving one of the criminal justice system's foundational tools for combating computer crime.